



## Version 3.0 Security Log's Training Guide

*Broadsword Program Office  
Air Force Research Laboratory / IFED  
315-330-4429*

37-3.0-TRNGSEC-10 00-00

16 October 2000

A banner for Security V 3.0. On the left, the "Broadsword" logo is shown. On the right, the text "Security" is displayed in a large, bold font, with "V 3.0" underneath it. The background is a dark, stylized illustration of a castle or fortress.

## What is ISSO ?

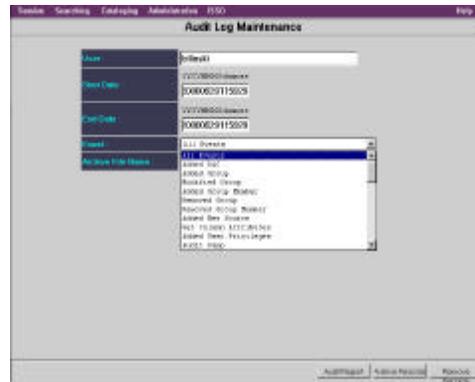
The ISSO function is used to view, archive, or remove audit information from the Broadsword Sybase Data Base based on the user(s), date/time and audit event.

## How do I query for information on a user ?

Parameter	Value
User Account	
Start Date	SYSTEM
End Date	SYSTEM
Event	SYSTEM
Archive File Name	SYSTEM

The ISSO can view, archive, or remove audit information from the Broadsword interface by clicking on the Audit Logs Maintenance screen from the Audit Logs menu. The Audit Log Maintenance screen contains a table of parameters. The first four parameters are used to query for the audit information, the last parameter is used when archiving the audit information. The first field, User Account, is used to query for audit information from a specific user. The default setting: Blank field; indicates all user accounts are being queried for audit information. The Start date/time indicates a query for **all** dates that start on that date for the given user on the chosen event. The End date/time of the audit information being queried indicates a query for **all** dates that end on that date for the given user on the chosen event. The default is when the start and end dates are the same, the interface will search for events on any date. The Event field lists all the events the system can query for. Archive File Name is the name of the file to which the audit records are being archived.

## What types of information can I query for?



The event drop box shows a listing of all the audit events that the ISSO can select for the audit report. The possible entries are All Events, Added DAC (Discretionary Access Code), Added Group, Added Group Member, Removed Group, Removed Group Member, Added New Source, Added User Privileges, Admin Lock, Admin Unlock, Audit Dump, Get Audit Archive List, Delete Audit, Gatekeeper Started, Gatekeeper Stopped, Got Audit Report, Modified Element, Query, Remove DAC, Remove Source, Remove Remote Gatekeeper, Remove User Privileges, Set Source Parameter, Set User DAC, Transfer Request, Catalog Request, User Logger In, User Logged Out, Clear Statistics, Accept Registration From Remote Gatekeepers, Register Our Gatekeeper With Keymaster, Update Daemon Status, New or Updated Gatekeeper Info. The default is All Events.

## How do I generate an Audit Report?

User	bilinski
Start Date	17/10/2011 13:59
End Date	17/10/2011 13:59
Event	Event: Success on
Output File Name	

In the example the ISSO for our local system wants to get a report on user 'bilinski'; in particular he wants a record of every log-in attempt by this user. All the ISSO needs to do is click the Audit Report button. The Audit Report button will request an audit report for viewing based on the query parameters selected above.

## How do I view the Audit Report?

Field	Value
User	Shelvis
Audit Date	01/01/2000 00:00:00
Audit Date	01/01/2000 00:00:00
Event	None Selected
Archive File Name	

[View Audit Report](#)

Audit Report   Archive Report   Search

When the ISSO clicks the Audit Report button the following screen will appear . By clicking on the “View Audit Report” link, the ISSO can view the audit report generated by the criteria specified.

## What does my Audit Report look like?

This is the report header.  
It contains all of the audit log criteria specified in the previous screen.

### Audit Report

User: bilinski for All Dates For User Logged In.

```
Login: bilinski IP: 255.255.255.255 Origin: Login: bilinski Gtkpr: 255.255.255.255 Session Keys: 1212
LOGIN @ 255.255.255.255 : Successful Login from aleph Gatekeeper
Login: bilinski IP: 255.255.255.255 Origin: Login: bilinski Gtkpr: 255.255.255.255 Session Keys: 1212
LOGIN @ 255.255.255.255 : Successful Login from aleph Gatekeeper
Login: bilinski IP: 255.255.255.255 Origin: Login: bilinski Gtkpr: 255.255.255.255 Session Keys: 1212
LOGOUT 255.255.255.255 : Gatekeeper timed out from Gatekeeper
```

This is a sample log entry.  
Each entry contains the username, IP Address, Gatekeeper, and Session Key, as well as all of the events that were audited.

This is a sample audit report generated by the “Audit Log Maintenance” page. This is the log generated by the previous request. The header contains all of the log criteria, and the rest contains log entries.

## How do I Archive a Report?

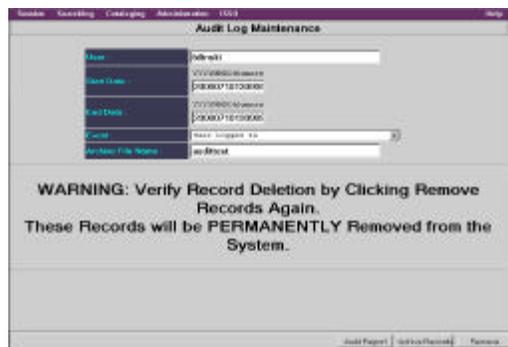
The screenshot shows a web browser window with the title "Audit Log Maintenance". The page has a navigation menu at the top with links for "Home", "Reporting", "Cataloging", "Administration", "SSO", and "Help". The main content area contains a form with the following fields:

Issue	336604
Start Date	YYYYMMDDHHMMSS
End Date	YYYYMMDDHHMMSS
Owner	User Support 10
Archive File Name	audittest

Below the form, there is a message: "Archive records(s) successfully." At the bottom of the page, there are three buttons: "Audit Package", "Archive Package", and "Review Package".

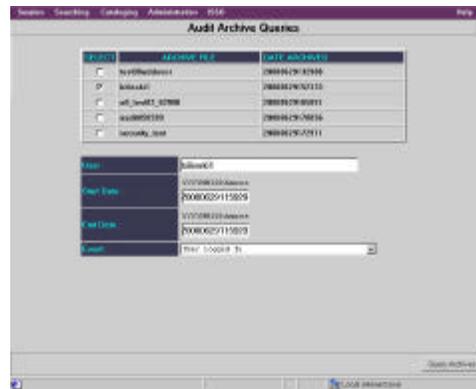
This screen is a result of clicking the “Archive Records” button on the “Audit Log Maintenance” page. In this example the ISSO wants to archive the report that he just generated. By clicking on the “Archive Records” button, the ISSO can archive the report into a file specified in the Archive File Name field. In this case, the archive file is named audittest.

## How do I remove a Record?



Now that the ISSO has archived these records, he or she now wants to remove the audits from the system. The ISSO then clicks the “Remove Records” button in the lower right corner and this confirmation screen appears. Clicking on the “Remove Records” button again will confirm the removal. Note that the you are NOT deleting records stored in the Archive File Name, but rather are deleting all of the pertinent records from the systems audits..

## Where are the files I have Archived?



The ISSO desires to check the archived file “bilinski1” for anytime the user “bilinski1” logged in. To access this this screen the ISSO must choose the Archived Logs function from the ISSO menu. To generate the report, the ISSO would click the Query Archives button. Note, that more than one archived file may be chosen.

## Where are the files I have Archived continued..



After the ISSO clicks the Query Archives button, the screen reloads displaying the View Audit Report hyperlink. The ISSO may then click on this hyperlink to review the report.